TechNote

SonicOS | Hub and Spoke TZ170 VPNs with Checkpoint NG

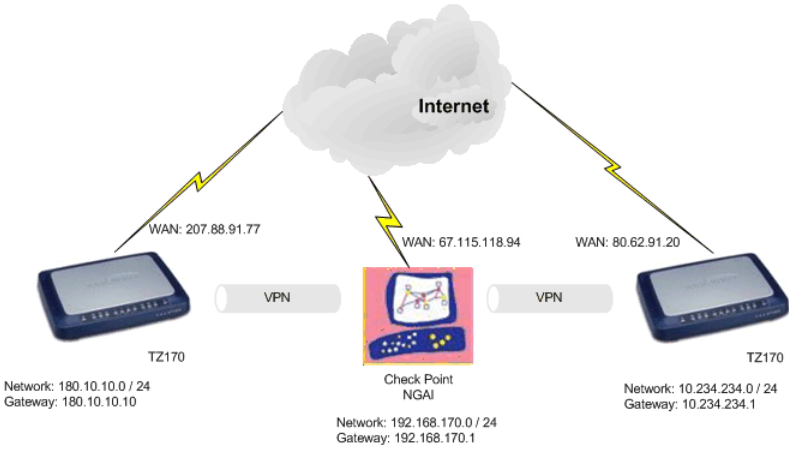
Introduction

This technote will detail all steps to get a Hub and Spoke setup between the SonicWALL SonicOS Enhanced and the Checkpoint NG. Within this setup the Checkpoint NG will be the HUB and 2 TZ170 units will be the Spokes.

Versions Used

- SonicOS 2.5.0.2 Enhanced on both TZ170 units
- Checkpoint FW-1 NGAI

Sample Diagram



Tasklist

On the SonicWALL units:

- Create new network objects and groups
- Create new VPN Policy for the Check Point FW-1 NG
- Specify Destination Network(s), IKE Phase 1 and Phase 2 properties

On FireWall-1 NG:

- Create local(Check Point) LAN network objects and group
- Create remote(SonicWALL's) LAN network objects
- Create new Interoperable Device objects
- Edit the Check Point Gateway object
- Verify the Topology
- Manually define VPN Domain
- Create new VPN Star Community
- Edit VPN Star community properties
- Verify Security Rules
- Verify Address Translation Rules

Testing

- Verify that traffic flows through the tunnel.
- Verify that applications function properly through the tunnel.
- Verify that the tunnel can reestablish if either side is disconnected.
- Verify that the network map and documentation match the running configuration.

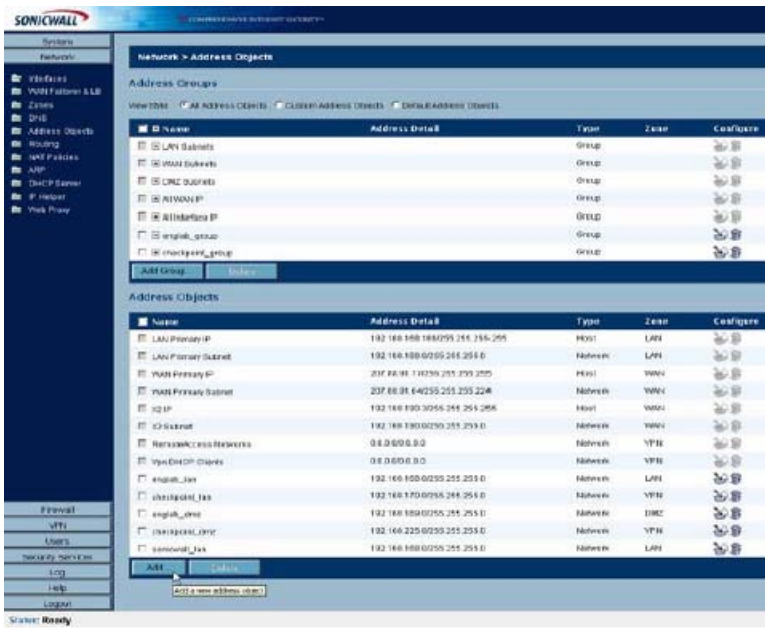
Before You Begin

If you have not already done so, set up a management system connecting to the SonicWALL's internal LAN interface. The SonicWALL should already be configured for internet access; if not, do this before completing any further steps. The Check Point FireWall-1 NG server is also assumed to be properly configured for internet access.

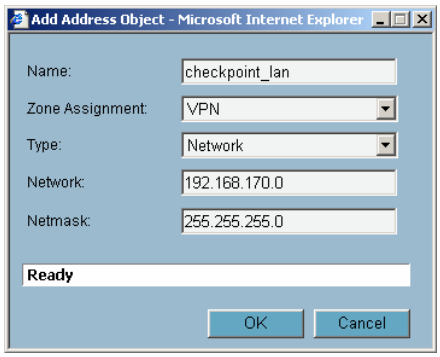
Setup Steps

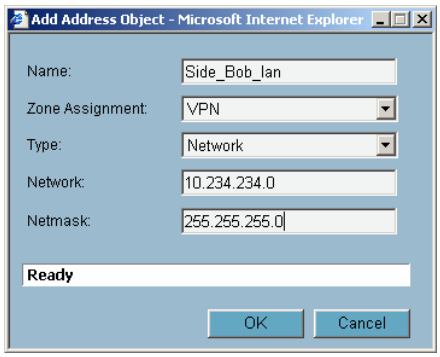
SonicWALL Setup Side Alice
Log into the SonicWALL's Management GUI using a current web browser.

The address objects will be created first, and then a group will be created to contain the address objects. From the navigation bar on the left, click on 'Network' and then 'Address Objects', this will bring up the 'Network > Address Objects' page. In the 'Address Objects' section, click on 'Add' to create the address objects for the networks connected to the Check Point FireWall-1 and SonicWALL. The first address object is for the LAN behind the Check Point FW-1.



Next create an address object group for the two checkpoint address objects. On the ‘Network > Address Objects’ page in the ‘Address Groups’ section, click on ‘Add Group…’ to create the address group for the objects.

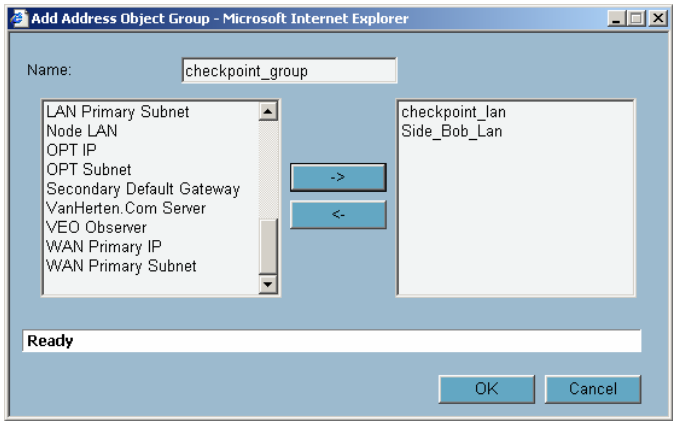




Name: checkpoint_lan
Zone Assignment: VPN
Type: Network
Network: 192.168.170.0
Netmask: 255.255.255.0
Click ‘OK’ to finish.

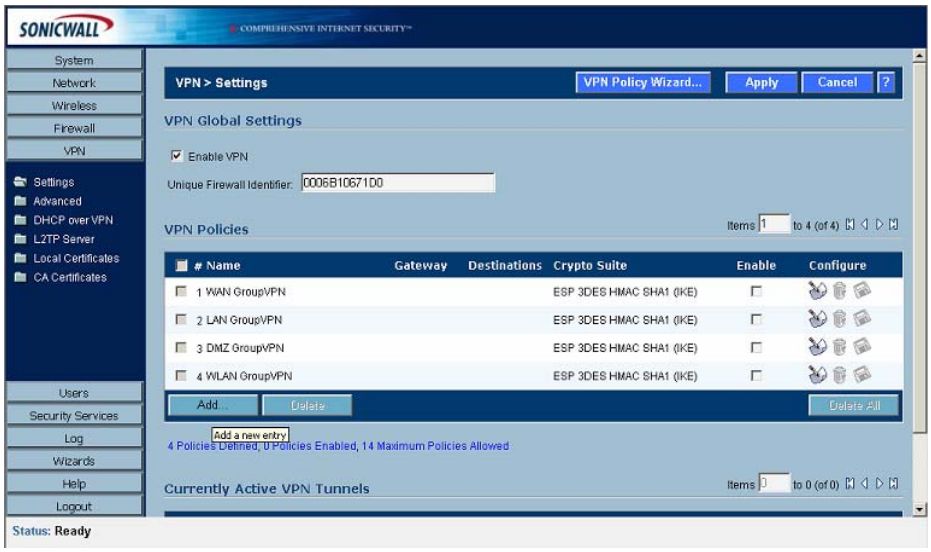
Name: Side_Bob_lan
Zone Assignment: VPN
Type: Network
Network: 10.234.234.0
Netmask: 255.255.255.0
Click ‘OK’ to finish.

Next create an address object group for the two checkpoint address objects. On the ‘Network > Address Objects’ page in the ‘Address Groups’ section, click on ‘Add Group…’ to create the address group for the objects. The ‘Name;" is "checkpoint_group"

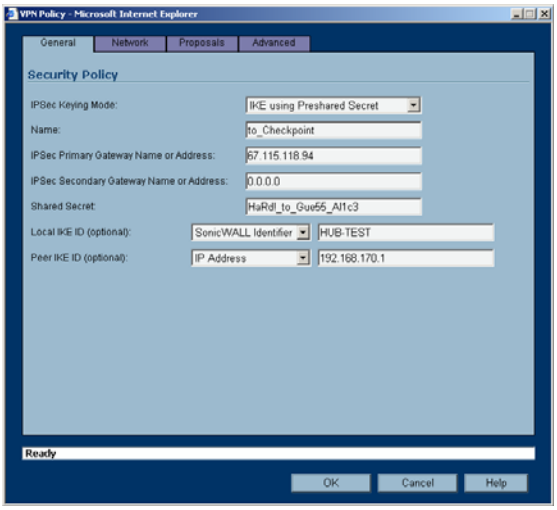


Select the "checkpoint_lan" object and ‘Ctrl’ or ‘Shift’ click to select the "Side_Bob_lan" object. Click the right arrow button to add both objects to the group.

From the navigation bar on the left, click on ‘VPN’, this will bring up the ‘VPN > Settings’ page. In the ‘VPN Global Settings’ section, make sure the ‘Enable VPN’ radio button is selected. In the ‘VPN Policies’ section, click on ‘Add’ to create the new VPN policy for the Check Point FireWall-1.

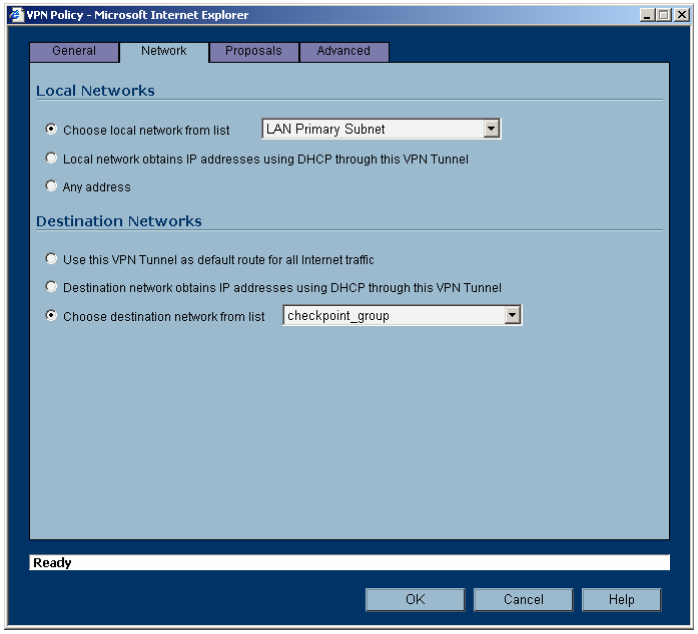


The ‘VPN Policy’ window will then appear. On the ‘General’ tab page, ‘Security Policy’ section, select “IKE using Preshared Secret” from the ‘IPSec Keying Mode:’ dropdown box.



Name: "to_checkpoint"
IPSec Primary Gateway Name or Address: 67.115.118.94
Shared Secret: HaRd!_to_Gue55_Al1c3
Local IKE ID: SNWL Identifier HUB-TEST (the SonicWALL Identifier needs to be identical as the VPN SA name on the CheckPoint NG)
Peer IKE ID: IP Address 192.168.170.1

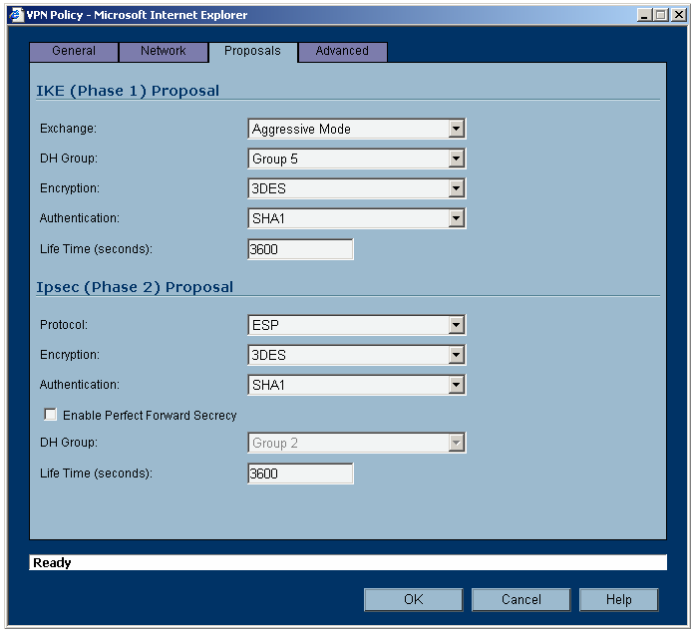
Next select the ‘Network’ tab.



In the ‘Local Networks’ section, select the radio button next to ‘Choose local network from list’ and select "LAN Primary Subnet" from the dropdown box.

In the ‘Destination Networks’ section, select the radio button next to ‘Choose destination network from list’ and select "checkpoint_group" from the dropdown box.

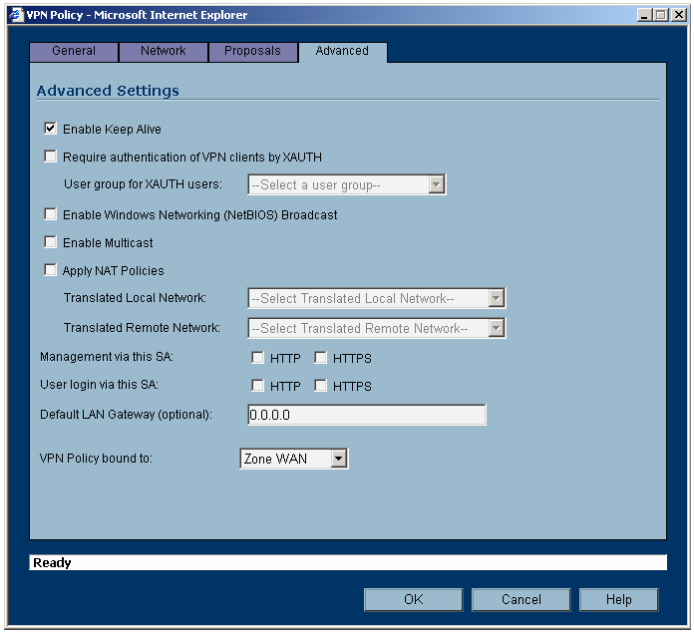
Next select the ‘Proposals’ tab. The default values should be correct, except the ‘Life Time’; normally "28800" should be lowered to "3600" in both Phase 1 and 2 proposals. Verify that all values are correct.



IKE (Phase 1) Proposal
Exchange: Aggressive Mode
DH Group: Group 5
Encryption: 3DES
Authentication: SHA1
Life Time (seconds): 3600

Ipsec (Phase 2) Proposal
Protocol: ESP
Encryption: 3DES
Authentication: SHA1
DH Group Group 2
Life Time (seconds): 3600
Do not enable Perfect Forward Security.

Next select the 'Advanced' tab.

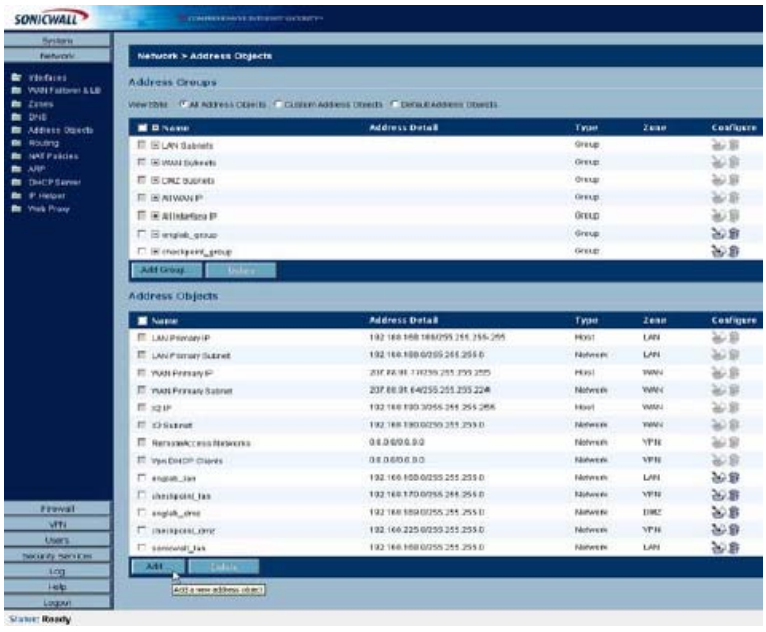


Make sure that the option Enable Keep Alive is checked. All other options can be left as they are. Click the OK button.

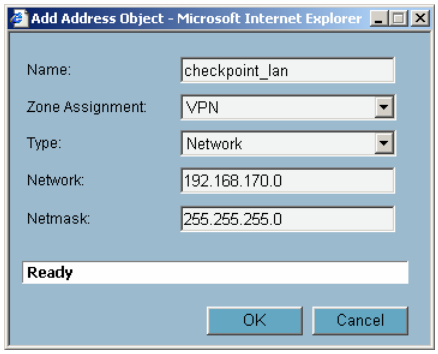
This completes the settings on the SonicWALL TZ170 installed on Side Alice. Now, we will setup the Check Point unit we will setup the TZ170 unit at Side Bob.

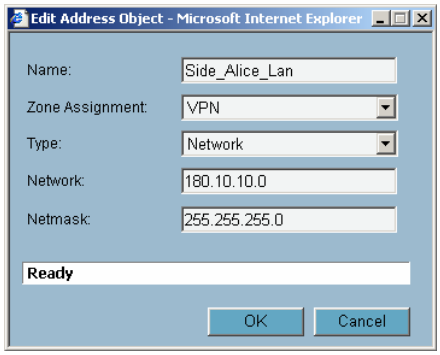
SonicWALL Setup Side Bob
Log into the SonicWALL's Management GUI using a current web browser.

The address objects will be created first, and then a group will be created to contain the address objects. From the navigation bar on the left, click on 'Network' and then 'Address Objects', this will bring up the 'Network > Address Objects' page. In the 'Address Objects' section, click on 'Add' to create the address objects for the networks connected to the Check Point FireWall-1 and SonicWALL. The first address object is for the LAN behind the Check Point FW-1.



Next create an address object group for the two checkpoint address objects. On the 'Network > Address Objects' page in the 'Address Groups' section, click on 'Add Group…' to create the address group for the objects.

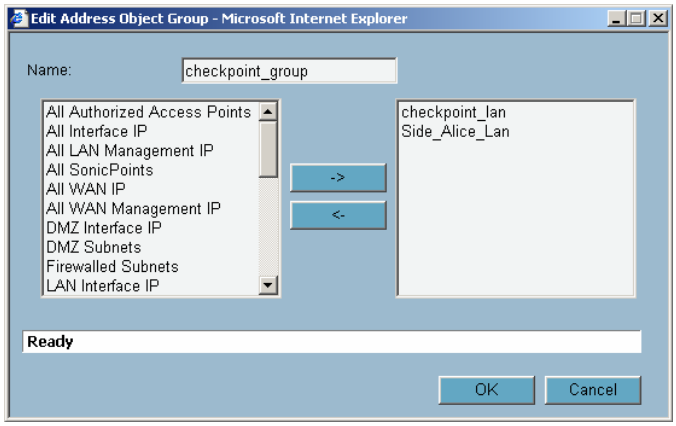




Name: checkpoint_lan
Zone Assignment: VPN
Type: Network
Network: 192.168.170.0
Netmask: 255.255.255.0
Click ‘OK’ to finish.

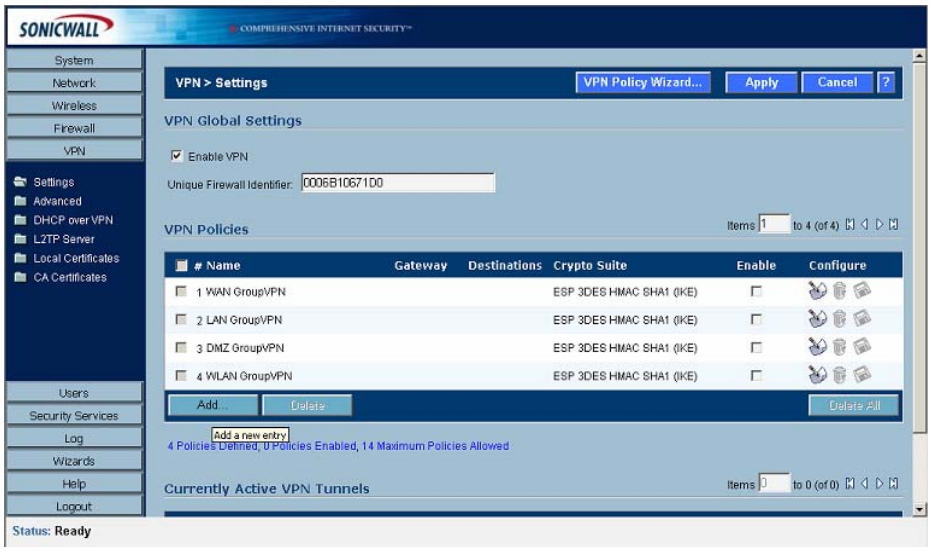
Name: Side_Alice_lan
Zone Assignment: VPN
Type: Network
Network: 180.10.10.0
Netmask: 255.255.255.0
Click ‘OK’ to finish.

Next create an address object group for the two checkpoint address objects. On the ‘Network > Address Objects’ page in the ‘Address Groups’ section, click on ‘Add Group…’ to create the address group for the objects. The ‘Name;" is "checkpoint_group"

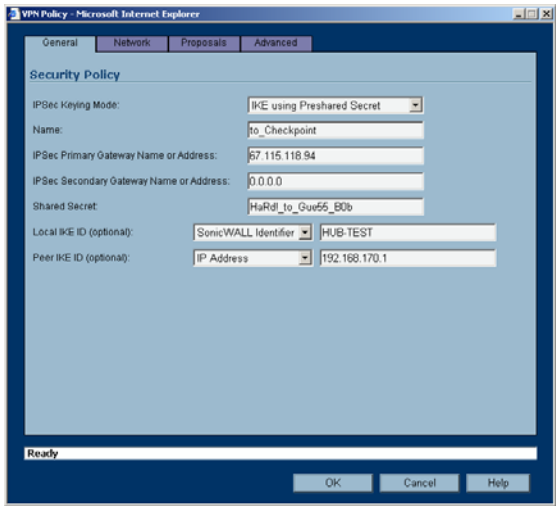


Select the "checkpoint_lan" object and ‘Ctrl’ or ‘Shift’ click to select the "Side_Alice_lan" object. Click the right arrow button to add both objects to the group.

From the navigation bar on the left, click on ‘VPN’, this will bring up the ‘VPN > Settings’ page. In the ‘VPN Global Settings’ section, make sure the ‘Enable VPN’ radio button is selected. In the ‘VPN Policies’ section, click on ‘Add’ to create the new VPN policy for the Check Point FireWall-1.

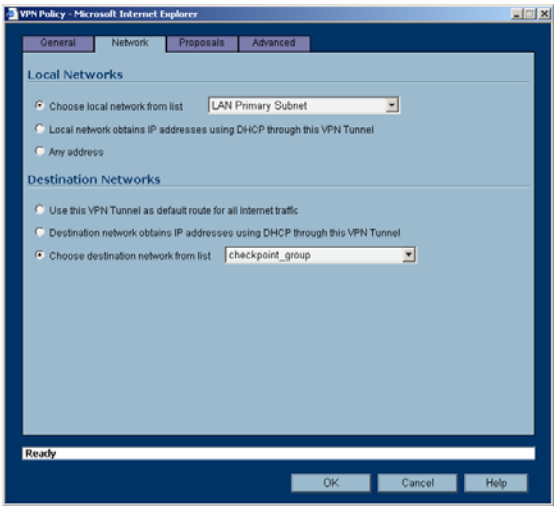


The ‘VPN Policy’ window will then appear. On the ‘General’ tab page, ‘Security Policy’ section, select “IKE using Preshared Secret” from the ‘IPSec Keying Mode:’ dropdown box.



Name: "to_checkpoint"
IPSec Primary Gateway Name or Address: 67.115.118.94
Shared Secret: HaRd!_to_Gue55_B0b
Local IKE ID: SNWL Identifier HUB-TEST
(the SonicWALL Identifier needs to be identical as the VPN SA name on the CheckPoint NG)
Peer IKE ID: IP Address 192.168.170.1

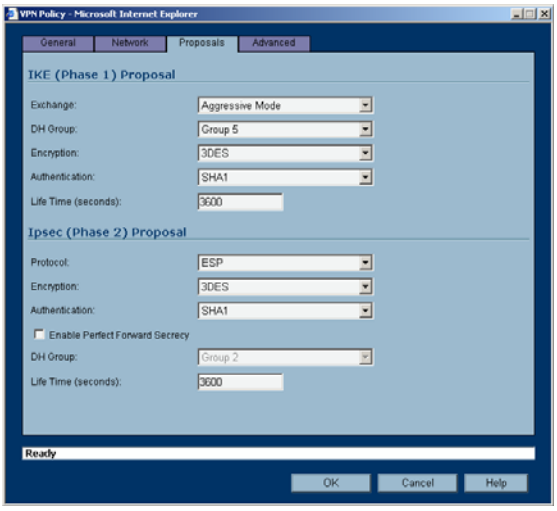
Next select the ‘Network’ tab.



In the ‘Local Networks’ section, select the radio button next to ‘Choose local network from list’ and select "LAN Primary Subnet" from the dropdown box.

In the ‘Destination Networks’ section, select the radio button next to ‘Choose destination network from list’ and select "checkpoint_group" from the dropdown box.

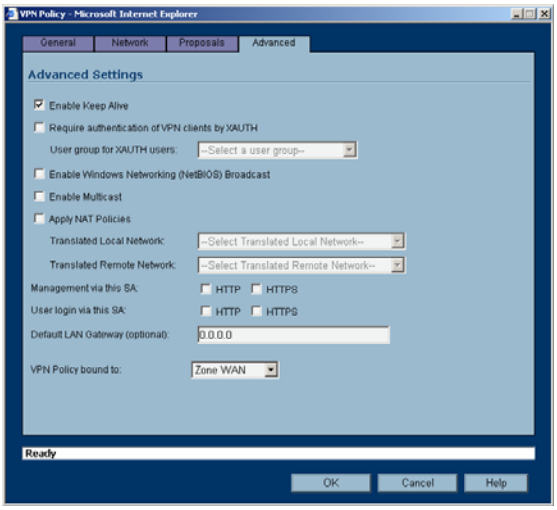
Next select the ‘Proposals’ tab. The default values should be correct, except the ‘Life Time’; normally "28800" should be lowered to "3600" in both Phase 1 and 2 proposals. Verify that all values are correct.



IKE (Phase 1) Proposal
Exchange: Aggressive Mode
DH Group: Group 5
Encryption: 3DES
Authentication: SHA1
Life Time (seconds): 3600

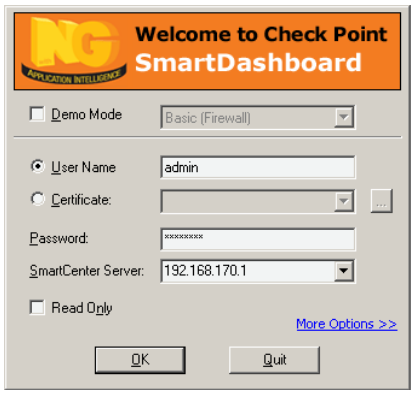
Ipsec (Phase 2) Proposal
Protocol: ESP
Encryption: 3DES
Authentication: SHA1
DH Group Group 2
Life Time (seconds): 3600
Do not enable Perfect Forward Security.

Next select the 'Advanced' tab.

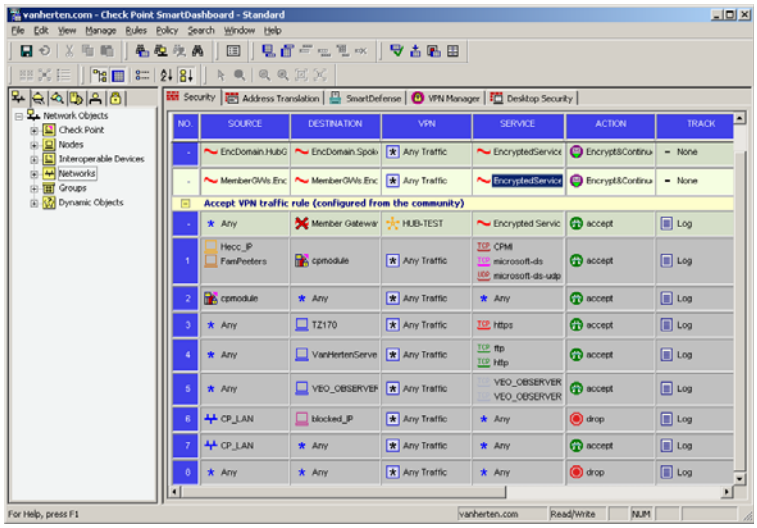


Make sure that the option Enable Keep Alive has been checked. All other options can be left as they are. Click the OK button.
This completes the settings on the SonicWALL TZ170 installed on Side Bob.

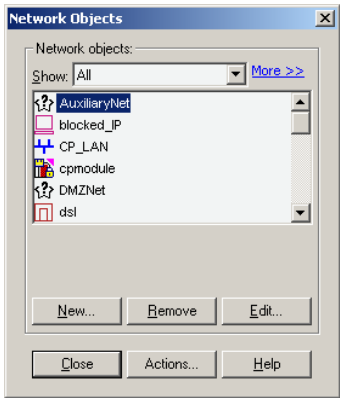
Check Point FireWall-1NG Setup
Log into SmartDashboard.



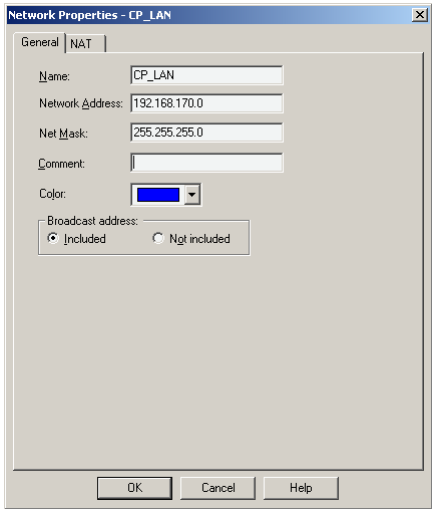
Before the VPN can be setup it is necessary to create Network Objects for all devices and networks. To create the network objects, first click on 'Manage' on the top of the SmartDashboard. Then click on 'Network Objects…' from the drop down box.



The 'Network Objects' window will then appear. The first object to create is for the LAN subnet of the Checkpoint FW, it's likely that these object already exist as they are used as the base for most rules. To create the LAN object, click the 'New' button at the bottom of the 'Network Objects' window, then select 'Network' from the dropdown box.



The ‘Network Properties’ window will then appear.



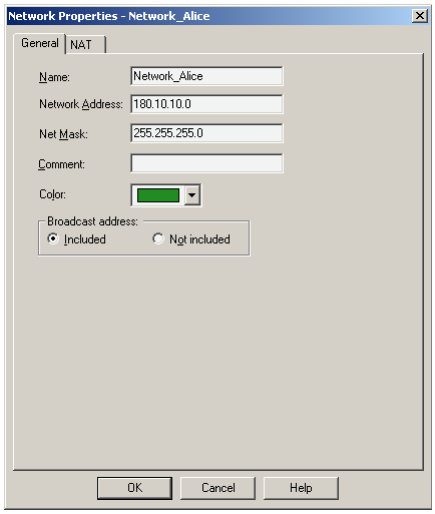
In this window, enter the object:

Name: CP_LAN
Network Address: 192.168.170.0
Net Mask: 255.255.255.0

The next network objects to create are for the LAN of the SonicWALL appliance at Side Alice and for the LAN of the SonicWALL appliance at Side Bob.
From the ‘Network Objects’ window, click the ‘New’ button at the bottom of the ‘Network Objects’ window, then select ‘Network…’ from the dropdown box.

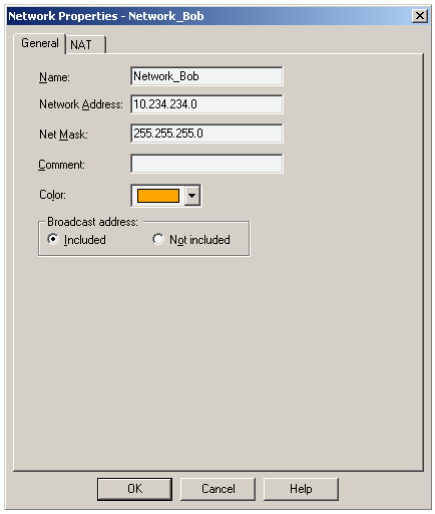
Here we create the Network Object for the LAN of Side Alice. Make sure that the Object contains the correct LAN Network Address and Net Mask. Within our example we used:

Name: Network_Alice
Network Address: 180.10.10.0
Net Mask: 255.255.255.0

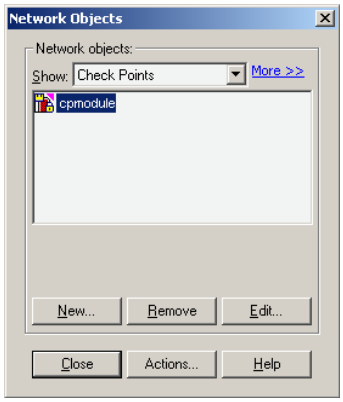


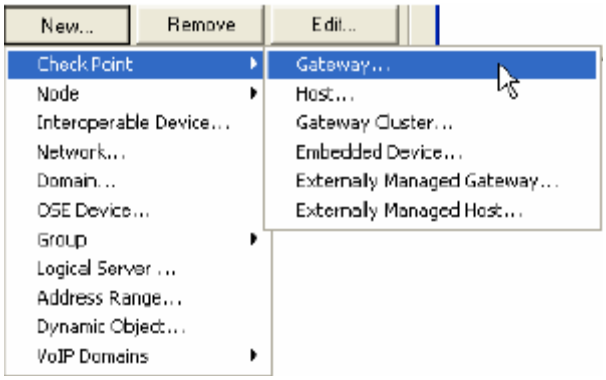
Here we create the Network Object for the LAN of Side Bob. Make sure that the Object contains the correct LAN Network Address and Net Mask. Within our example we used:

Name: Network_Bob
Network Address: 10.234.234.0
Net Mask: 255.255.255

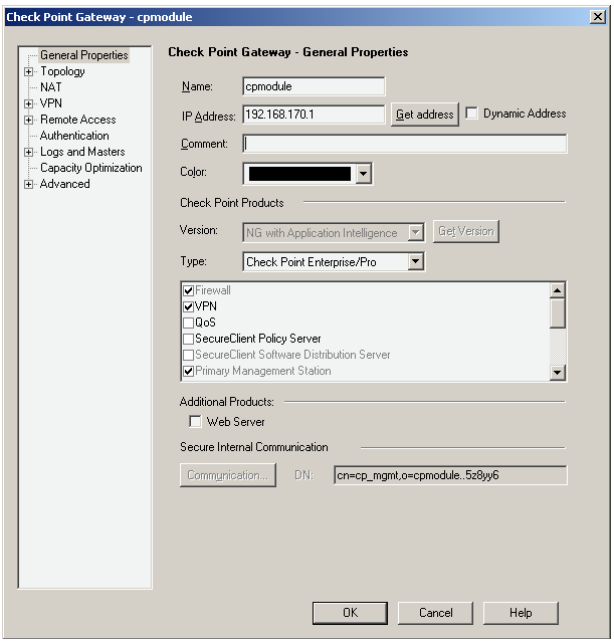


Next, edit the 'Check Points' network object. It should be named the same as the machine name then press the edit button. If it does not exist, create it under 'New' > 'Check Point' > 'Gateway…' and proceed to the next step.

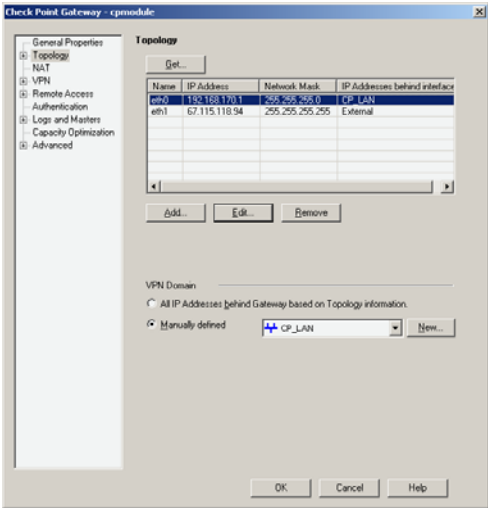




The ‘Check Point Gateway’ page will appear. On ‘General Properties’, verify the ‘IP Address’ and that both ‘FireWall-1’ and ‘VPN-1 Pro’ are selected. In this example, the ‘IP Address’ is “192.168.170.1”. When finished, click ‘Topology’ on the left hand side.



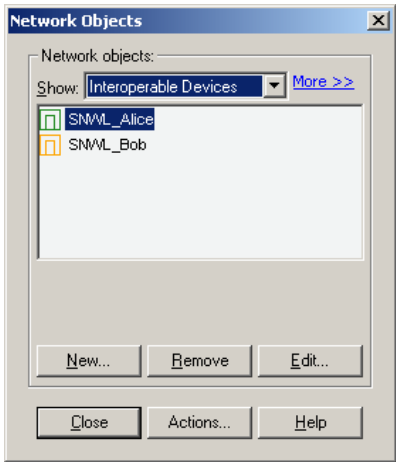
On ‘Topology’, verify the network addresses of the ‘internal’ and ‘external’ networks listed under the ‘Topology’ section. If nothing is populated in the topology fields, click ‘Get Topology…’

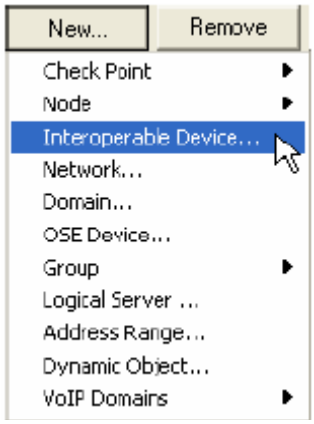


In this example:
External network: “67.115.118.94”
Net mask : “255.255.255.255”
Internal network: “192.168.170.1”
Net mask: “255.255.255.0”
(internal is also referred to as ‘This Network’).

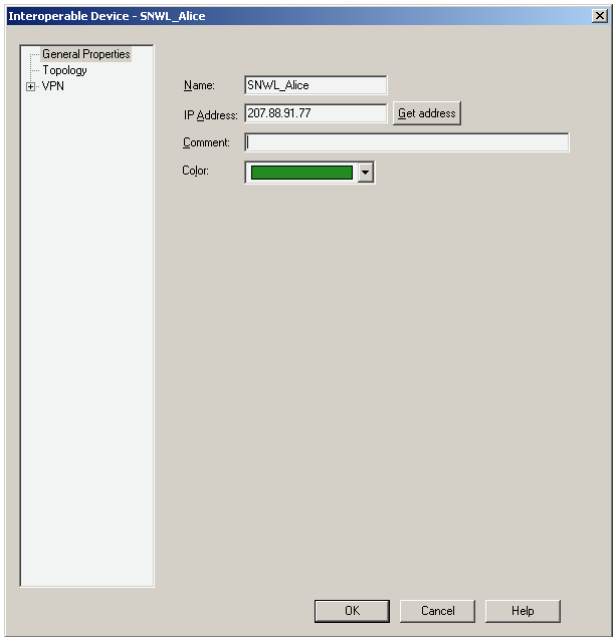
In the ‘VPN Domain’ section select ‘Manually defined’ and select the previously created “CP_LAN” Network Object with the dropdown menu. When this is done you can close this page by pressing the OK button.

It is needed to create also Interoperable Network objects for the both SonicWALL appliances. Go to ‘Manage’ > ‘Network Objects’ now the Network Objects window will then appear. To create the ‘Interoperable Device’ object, click the ‘New’ button at the bottom of the ‘Network Objects’ window, then select ‘Interoperable Device’ …’ from the dropdown box. The ‘Interoperable Device’ window will then appear.





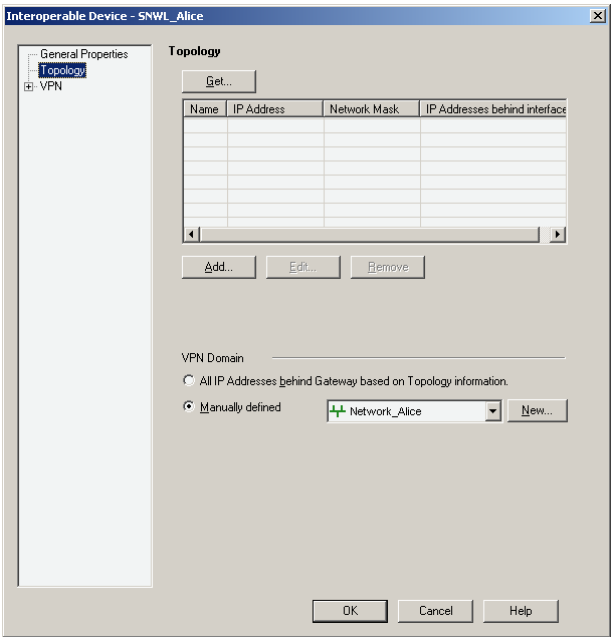
In this window, under ‘General Properties’ enter
Name: SNWL_Alice
IP Address: 207.88.91.77
Next click ‘Topology’ on the left hand side.



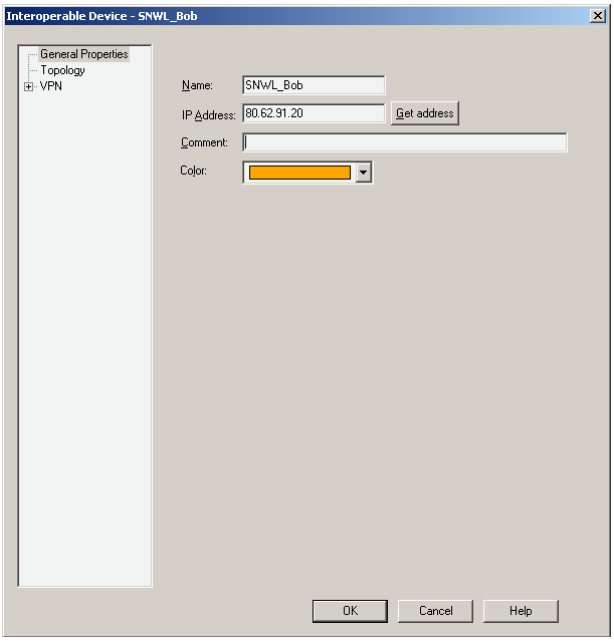
.

On the ‘Topology’ page, under the ‘VPN Domain’ section, select ‘Manually defined’ and select the previously created “Network_Alice” Network Object with the dropdown menu. Click on ‘OK’ to finish.

An Interoperable Device Object needs also to be created for Side Bob. Go to ‘Manage’ > ‘Network Objects’ now the Network Objects window will then appear. To create the ‘Interoperable Device’ object, click the ‘New’ button at the bottom of the ‘Network Objects’ window, then select ‘Interoperable Device’ …’ from the dropdown menu.

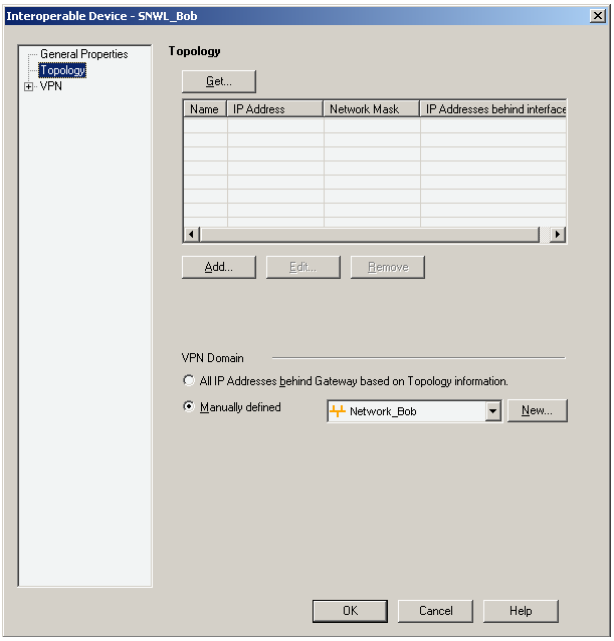


The ‘Interoperable Device’ window will then appear.

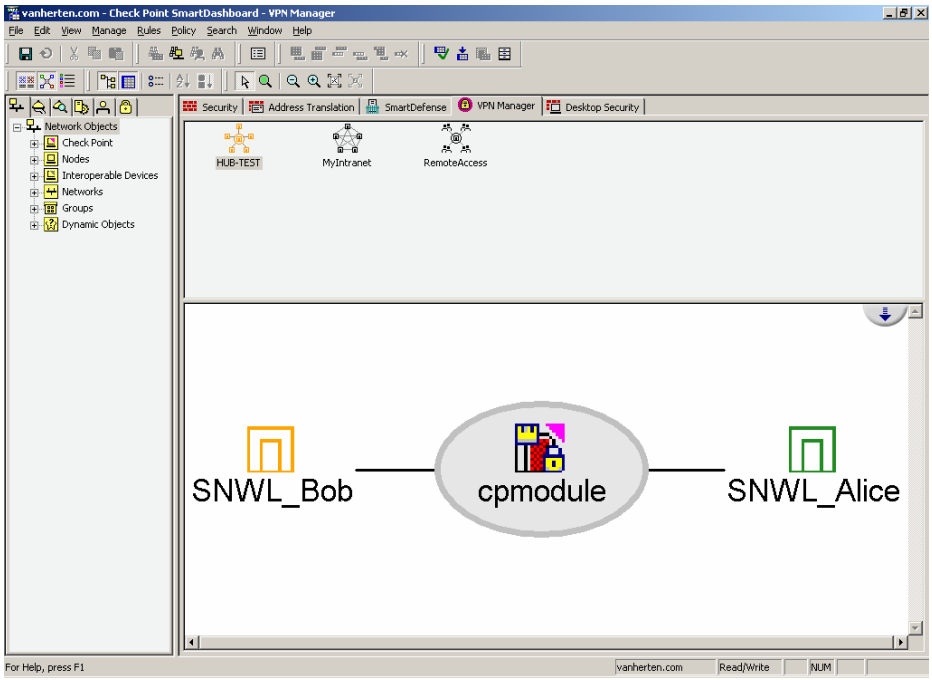


In this window, under ‘General Properties’ enter:
Name: SNWL_Bob
IP Address: 80.62.91.20
Next click ‘Topology’ on the left hand side.

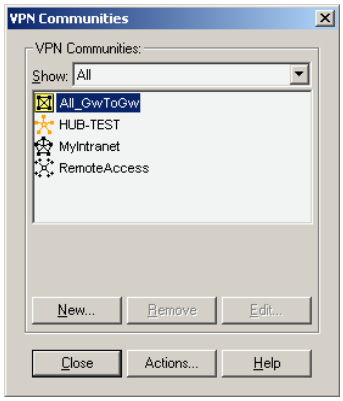
On the ‘Topology’ page, under the ‘VPN Domain’ section select ‘Manually defined’ and select the previously created “Network_Bob” Network Object with the dropdown menu. Click on ‘OK’ to finish.



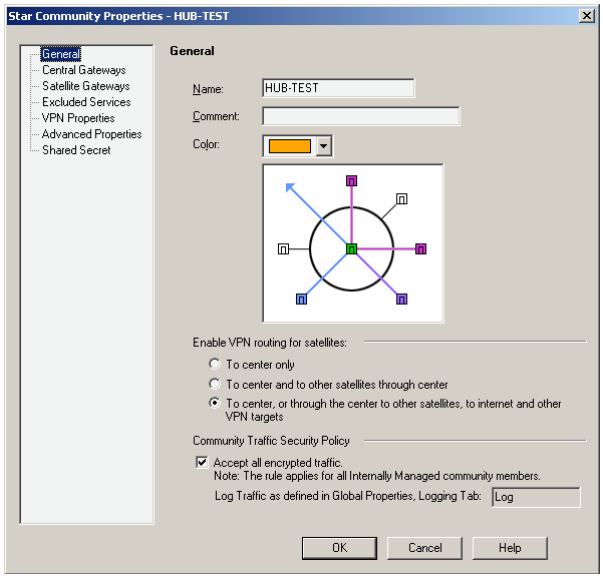
Now all the Network Addresses are created which will be needed to setup the VPN SA on the Checkpoint NGAI unit. Next, define the VPN. From the top menu, select ‘Manage’ and then ‘VPN Communities…’; the ‘VPN Communities’ window will appear.



From the ‘VPN Communities’ window, select the ‘New’ button on the bottom. Then select ‘Site To Site’ and ‘Star…’ The ‘Star Community Properties’ page will appear.



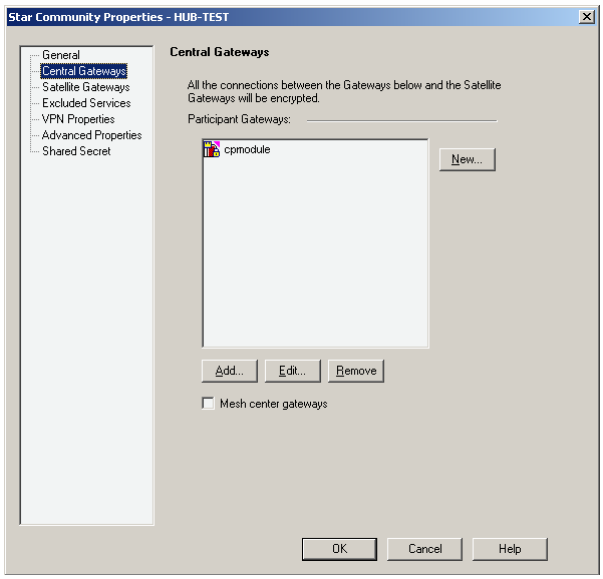
On the ‘Star Community Properties’ page, enter the VPN name in the ‘Name:’ field. In this example, the ‘Name:’ is "HUB-TEST" which needs to be the same as the SNWL Identifier setup in the VPN SA on the Spokes.

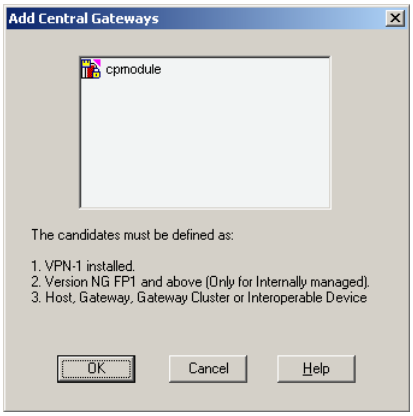


For the ‘Enable VPN routing for satellites’ you need to select the option ‘To center, or through the center to other satellites, to internet and other VPN targets. ’

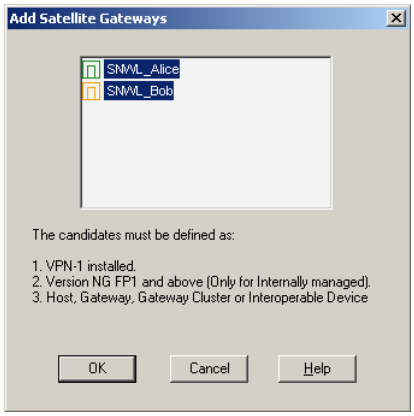
At the Community Traffic Security Policy it is necessary to have the checkbox ‘Accept all encrypted traffic’ ticked. Next, click on ‘Central Gateways’.

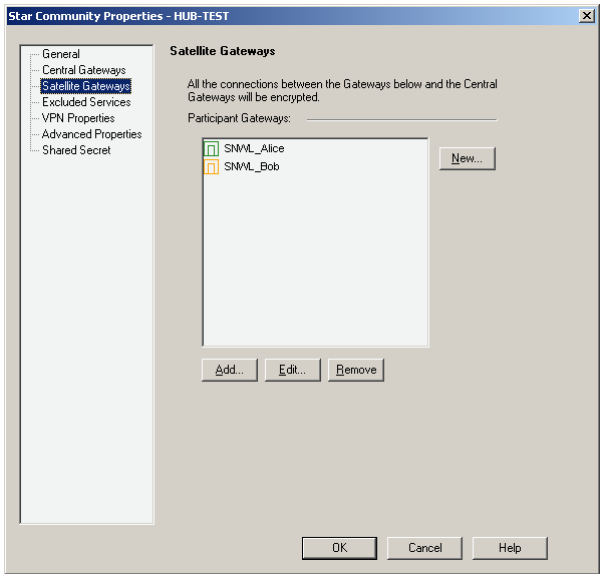
On the Central Gateways, click on the ‘Add…’ button under the ‘Central Gateways:’ section. This will bring up the ‘Central Gateways’ window. Select here the address object ‘cpmodule’ and press OK.





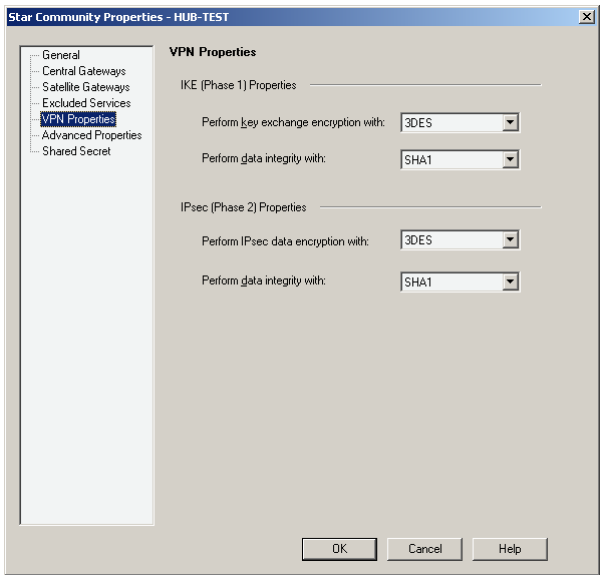
Next, click on 'Satellite Gateways'. On the Satellite Gateways, click on the 'Add…' button under the 'Satellite Gateways:' section. This will bring up the 'Satellite Gateways' window.





Select here the address objects 'SNWL_Alice' and address object 'SNWL_Bob' after this is done press OK.

Click on 'VPN Properties'.

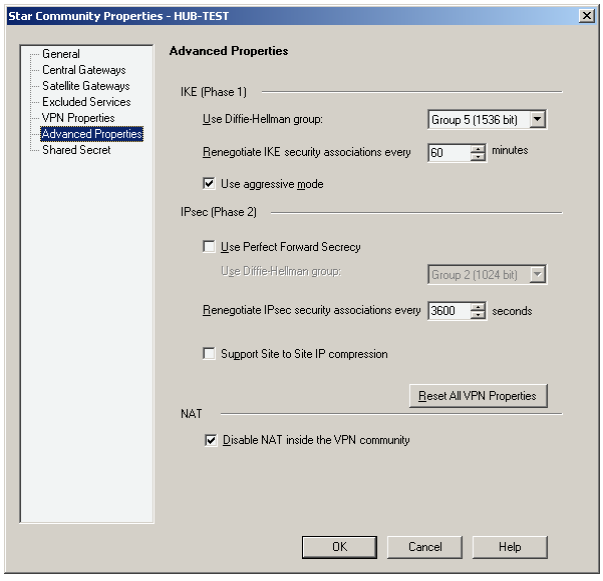


Enter the 'IKE (Phase 1) Properties' and the 'IPsec (Phase 2) Properties'. In this example, the 'IKE (Phase 1)' section the settings are as follows:

IKE (Phase 1) Properties
Perform key exchange encryption with: 3DES
Perform data integrity with: SHA1

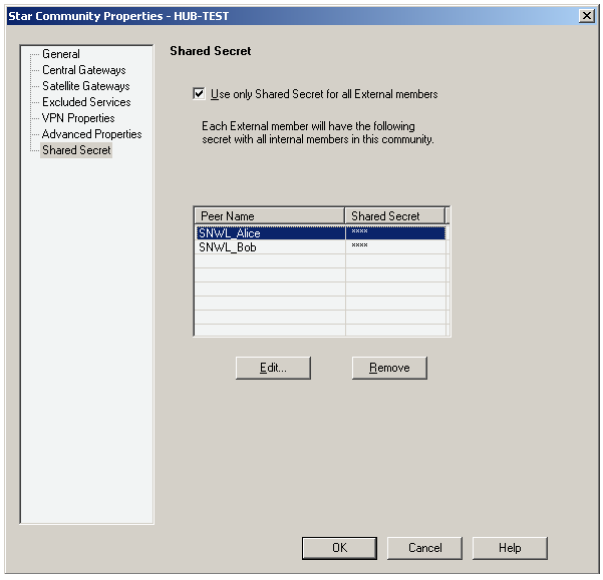
Ipsec (Phase 2) Properties
Perform IPsec data encryption with: 3DES
Perform data integrity with: SHA1

Next, click on 'Advanced Properties.'

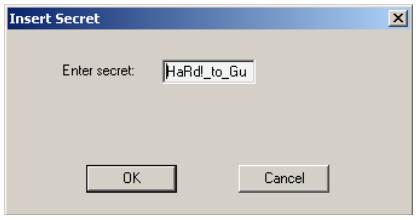


In the ‘Advanced Properties’ section, under IKE (Phase 1), modify the ‘Renegotiate IKE security associations every’ field to "60" minutes and the ‘Use Diffie-Hellman group’ should be "Group 5 (1536 bit). Tick the option ‘Use aggressive mode’ For the ‘Ipsec (Phase 2) Proposal’ section the settings are as follows: ‘Life Time (seconds)’ is "3600". Do not enable Perfect Forward Security. At the ‘NAT’ it is necessary to tick the option ‘Disable NAT inside the VPN community’

Click ‘Shared Secret’.



On the ‘Shared Secret’ section, tick the option ‘Use only Shared Secret for all External members’. Highlight "SNWL_Alice" in the ‘Peer Name’ table below. Click on the ‘Edit…" button to enter the secret. In this example, the shared secret is "HaRd!_to_Gue55_Al1c3" press the OK button. After this Highlight "SNWL_Bob" in the ‘Peer Name’ table below. Click on the ‘Edit…" button to enter the secret. In this example, the shared secret is "HaRd!_to_Gue55_B0b" and press the OK button.



Click ‘OK’ to finish the VPN Interoperability Hub Spoke setup between the SonicOS 2.5 Enhanced and Checkpoint NG within the SmartDashboard. Make sure that the Policy has been installed onto the Checkpoint firewall to have it working.

Document Created: 11/16/2004
Last Updated: 06/19/2008
Version 1.1